

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----	X	
PETERSEN ENERGÍA INVERSORA,	:	
S.A.U. AND PETERSEN ENERGÍA,	:	Case No. 1:15-cv-02739-LAP
S.A.U.,	:	
	:	
Plaintiffs,	:	
v.	:	
	:	
ARGENTINE REPUBLIC AND YPF	:	
S.A.,	:	
	:	
Defendants.	:	
-----	X	
ETON PARK CAPITAL	:	
MANAGEMENT, L.P., ETON PARK	:	
MASTER FUND, LTD. AND ETON	:	
PARK FUND, L.P.,	:	
	:	
Plaintiffs,	:	Case No. 1:16-cv-08569-LAP
v.	:	
	:	
ARGENTINE REPUBLIC AND YPF	:	
S.A.,	:	
	:	
Defendants.	:	
-----	X	

**EXPERT DECLARATION OF MIRIAM MABEL IVANEGA**

Pursuant to 28 U.S.C. § 1746 and Rule 44.1 of the Federal Rules of Civil Procedure, I, Miriam Ivanega, state the following:

1. Counsel for the Argentine Republic (the “Defendant”) have requested my opinion on certain questions of Argentine law relevant to a dispute between the Defendant and plaintiffs Petersen Energía Inversora, S.A.U. and Petersen Energía, S.A.U. (collectively, “Petersen”), and Eton Park Capital Management, L.P., Eton Park Master Fund, Ltd. and Eton Park Fund, L.P.

(collectively, “Eton Park” and together with Petersen, “Plaintiffs”) in the postjudgment discovery process in the above-captioned cases.

2. I am a duly licensed and authorized attorney in Argentina. I am a professor of Administrative Organization and Public Employment and Transparency, Compliance and Public Control of Public Procurement and Director of the Master's Degree in Administrative Law at the Law School of the Universidad Austral in the Autonomous City of Buenos Aires, Argentina.
3. I have a Master's in Administrative Law and a Doctorate in Law and Social Sciences. I am a Founding Member of the Ibero-American Forum of Administrative Law and of the International Association of Administrative Law, professor of graduate courses in law and lecturer in public and private universities in the Argentine Republic and in other Latin American countries (Peru, Ecuador, Colombia, Brazil, Uruguay, Mexico, Dominican Republic, El Salvador). I have published eleven books related to public law, on issues of public control, transparency in public procurement, liability of public officials, administrative organization and civil service, financial administration and public management. Among the positions that I have held in the public sector, I highlight having held the position of Authority of Application of the Public Ethics Law in the Magistrate Board of the Judiciary of the Autonomous City of Buenos Aires.

#### **EXECUTIVE SUMMARY**

4. I understand that Plaintiffs have requested that the Defendant collect and produce certain documents relating to the relationship between the Defendant and YPF S.A. (“YPF”) or Banco Central de la República Argentina (“BCRA”), including communications from certain persons who are or were officials of the national government.

5. In the first section of this report, I analyze whether under Argentine law emails and internal documents created or exchanged between Argentine government officials involving various devices under the possession, control or custody of the national government constitute public information to which persons outside the administration are entitled to access. First, the Defendant takes its actions by complying with a detailed set of rules and regulations. Any expression or activity that does not conform to such rules—including internal mailings and documents—is deliberative acts that does not have the character of government acts and therefore do not constitute “public information” as such concepts are defined in Argentine law. Only to the extent that the content of such internal communications gives rise to acts of decision and is included in the administration's actions that are recorded in the only system enabled for such purposes, the Electronic Document Management System (“GDE”), they become acts of government which, as a general rule, constitute public information. Second, even if communications and documents generated prior to an act of government could be considered public information, and their content be recorded in the GDE, the regime of the right of access to public information under Argentine law establishes certain limitations to the Defendant's obligation to provide information generated by it or its officials.
6. In the second section of this report, I analyze whether under Argentine law the Defendant could take possession, control or custody of personal devices and accounts of persons who are or were officials of the national government. Under Argentine law, such personal devices and accounts, as well as any content generated on or through them, are the private property of such officials and Defendant has no possession, control or custody of them. Under Argentine law, the Defendant has no legal standing to collect or deliver to third parties the personal devices and accounts without the express authorization of the owner of such devices and accounts.

Quite to the contrary, any officer of Defendant who accesses or takes possession of the personal devices or accounts of its officers or their contents would be guilty of the offenses set forth in Articles 153 and 153bis of the Argentine Criminal Code.

**I. E-MAILS AND INTERNAL DOCUMENTS CREATED OR EXCHANGED BETWEEN ARGENTINE GOVERNMENT OFFICIALS INVOLVING DIFFERENT DEVICES UNDER THE POSSESSION, CONTROL OR CUSTODY OF THE NATIONAL GOVERNMENT DO NOT CONSTITUTE PUBLIC INFORMATION TO WHICH PERSONS OUTSIDE THE ADMINISTRATION MAY HAVE ACCESS.**

7. The e-mails exchanged between Argentine government officials involving devices under the possession, control or custody of the national government, as well as internal working documents, do not constitute communications made through the system enabled by the National State for the management of administrative activity and, therefore, cannot be considered information to which third parties have access under the Argentine law on the right of access to public information. Both the National State and the identified officials have a legitimate interest in preserving the confidentiality of such information, and may not be compelled to disclose it.

**A. Internal communications and documents of Argentine officials, even when they involve devices under the possession, control or custody of the national government, are not “public information”.**

8. The functions of the State are developed through judicial, legislative or administrative procedures and processes that must comply with the respective regulations. In the case of the executive branch, the administrative procedure consists of all reports, orders, rulings and official documents in general that are the product of administrative proceedings (Law No. 19,549 as amended by Law No. 27,742, Decree No. 1759/1972 as amended by Decree No. 695/2024, Articles 7 and 8).

9. Administrative files are processed by electronic means, are decided by the action of the body to which a law or a decree has attributed jurisdiction and are formed with the orderly aggregation of documents, evidence, opinions, reports, agreements, notifications and other proceedings that are required to be included in them.
10. The different instances that reflect the will of the National State to generate an act of government must adopt a form established by regulation (Decree No. 336/2017). Today, administrative actions are channeled through the GDE which is a platform that implements electronic records management (Decree No. 695/2024, art. 7.c). The GDE was implemented in 2016 “as an integrated system of labeling, numbering, tracking and registration of movements of all acts and files of the National Public Sector.” (Decree No. 561/2016, arts. 1 and 2).
11. Consequently, in order for an official of the Defendant to manifest the will of the Argentine State by exercising administrative functions, including giving instructions or entering into agreements with entities that have their own legal personality (whether or not they have state participation), he or she must do so through an administrative procedure processed through the GDE, which is the only system enabled to do so.
12. Only those reports, rulings, orders, resolutions or other acts of the Administration that are incorporated in this procedural system can express the will of the State with respect to an act of government that is subject to the regime of publicity.<sup>1</sup> Decree No. 333/1985 —later replaced

---

<sup>1</sup> See SACRISTÁN, E. B., Acceso a la información: a propósito de los casos “PAMI” y “Giustiniani”, JA 2016-I, p. 31. The author understands that the access to public information regulation is limited to the issuers of government acts. Likewise, it refers to the principle of “publicity of government acts” and its link with the republican, representative and federal system established in Article 1 of the Argentine Constitution (cfr. GELLI, M. A., Constitución de la Nación Argentina Comentada y Concordada, 5th expanded and updated edition, Buenos Aires, La Ley, 2018, , Volume I., pp. 27-29).

by Decree No. 336/2017 in view of the technological modifications derived from the use of GDE— expressly provided that no type of documentation that did not comply with the rules provided for such purposes would be processed. For the purposes of public administration (and the issuance of acts of government) all such actions are not relevant. To the extent that they are not part of an act of the administration uploaded to GDE, e-mails and documents created or shared that are exchanged between Argentine government officials involving different devices under the possession, control or custody of the national government, constitute deliberative acts and working papers —mere exchanges— that cannot be identified as public information.<sup>2</sup>

13. In the Argentine Republic, under the regime of access to public information, individuals only have the right to request and obtain documents from the national government regarding acts of government only through a request for information under the procedure established by Law No. 27,275 on the Right of Access to Public Information and Regulatory Decree No. 206/2017(“DAIP”).<sup>3</sup>

14. The DAIP finds its basis in the conception that considers access to public information regarding acts of government as a fundamental right —an integral part of freedom of expression— of all citizens who wish to seek and receive information and data held by the State.<sup>4</sup> Consequently, Law No. 27,275 establishes the obligation of the Defendant to deliver documentation regarding

---

<sup>2</sup> Decree No. 780/2024, which amended Decree No. 206/2017 confirms the sense that preparatory deliberations and working papers, as well as the preliminary examination of a matter, are not considered documents of a public nature.

<sup>3</sup> This is without prejudice to the jurisdictional powers within the framework of criminal proceedings.

<sup>4</sup> See Articles 1, 14, 16, 31, 32 and 33 of the Argentine Constitution; Article 19 of the International Covenant on Civil and Political Rights and of the Universal Declaration of Human Rights, Article 13 of the American Convention on Human Rights and Article 4 of the American Declaration of the Rights and Duties of Man.

acts of government in response to a request made by a citizen in exercise of the DAIP as long as it refers to public information (Law No. 27,275, Articles 2 and 13).

15. Under Argentine law, for the purposes of the national public administration, public information is defined as any type of data contained in documents of any format that the officials of such administration, the subjects obliged to provide information, generate, obtain, transform, control or keep in the context of state activity. Until an act of government is verified, there is no public information.

16. A simple exegetical reading of Law No. 19,549 as amended by Law No. 27,742 and its Regulatory Decree (Decree No. 1759/1972, as amended by Decree No. 695/2024), Decree No. 336/2017 and Decree No. 561/2016, shows that internal emails exchanged between Argentine government officials involving devices under the possession, control or custody of the national government, as well as internal working documents that are not uploaded to the GDE system and do not constitute acts of government are not in the nature of public information. Consequently, the Defendant is not obliged to turn over such documents. Such obligation will only exist to the extent that the content of such internal communications or documents is reflected in a report, opinion, ruling, resolution or other acts of government through the GDE system.

**B. Even if internal government communications and documents involving devices in the possession, control or custody of the national government could be considered public information, the Defendant is exempted from its obligation to provide any information covered by the exceptions provided for in the Right of Access to Public Information Law.**

17. Even assuming that communications exchanged or documents prepared involving devices in the possession, control or custody of the national government and other internal documents

may be considered acts of government, the DAIP regime itself provides that certain information is not subject to public disclosure.

18. The Defendant is not required to disclose under the DAIP privileged information (excluded from the regime) because it is linked to the matters excluded from public access set forth in Article 8 of Law No. 27,275. Those legitimate restrictions are:

- a. Information expressly classified as reserved or confidential or secret for reasons of defense or foreign policy<sup>5</sup>;
- b. Information that could jeopardize the proper functioning of the financial or banking system;
- c. Industrial, commercial, financial, scientific, technical or technological secrets, the disclosure of which could harm the level of competitiveness or damage its interests;
- d. Information obtained confidentially that affects the rights or legitimate interests of a third party;
- e. Information held by the Financial Information Unit aimed at the prevention and investigation of assets derived from illegal activities;
- f. Information created by those who are dedicated to regulate or supervise financial institutions when they refer to situation examinations, evaluation of their operating system or condition of their operation;
- g. Information prepared by legal advisors or attorneys of the national public administration the disclosure of which could reveal the strategy to be adapted in the

---

<sup>5</sup> Defense or foreign policy are linked to national security, in a broad sense, which in a State must constitute a legitimate restriction on the right of access to public information, provided that it is established by law.



defense or prosecution of a judicial case or disclose the techniques or procedures for the investigation of any crime or other irregularity or when the information would deprive a person of the full exercise of the right to due process;

- h. Information protected by professional secrecy;
- i. Information containing personal data (cfr. Law No. 25,326 on Personal Data Protection);<sup>6</sup>
- j. Information that may cause danger to the life or safety of a person;
- k. Information of a judicial nature whose disclosure is prohibited by other laws or by commitments undertaken by the Defendant in international treaties;
- l. Classified information obtained in the course of an investigation, the disclosure of which could frustrate the success of an investigation; and
- m. Information relating to a corporation subject to the public offering regime.

19. In the event of a request made by a citizen in exercise of the DAIP that falls under any of the exceptions set forth in Article 8 of Law No. 27,275, the State is exempted from the obligation to provide information.<sup>7</sup>

## **II. THE DEFENDANT DOES NOT HAVE AND CANNOT TAKE POSSESSION, CONTROL OR CUSTODY OF THE DEVICES AND PERSONAL ACCOUNTS OF CURRENT AND FORMER OFFICIALS OF THE ARGENTINE GOVERNMENT.**

### **A. In the absence of an act of Congress or a court order from an Argentine court authorizing it, the Argentine Republic cannot access the private devices or**

<sup>6</sup> Article 5 of Law No. 25,326 specifies as a principle that the processing of personal data is unlawful when there is no consent of the owner. Consequently, Article 7 establishes that no one may be forced to provide sensitive data, establishing only two exceptions to this principle: when there are reasons of general interest authorized by law or when its use is linked to statistical or scientific purposes when the owners cannot be identified.

<sup>7</sup> The only case in which these exceptions are not applicable is expressly provided for in Article 8, last paragraph, and refers to “cases of grave violations of human rights, genocide, war crimes or crimes against humanity”.

**private communications of its citizens without directly violating the National Constitution.**

20. The devices (with their contents) and personal email accounts to which Plaintiffs seek access are not in the possession, control or custody of the Defendant. On the contrary, they are the exclusive property of their owners. Both those devices and their contents — to the extent they have not been made public by their legitimate owners — constitute for the Defendant the property of another.
21. Article 17 of the National Constitution (“Argentine Constitution”) provides that “[p]roperty is inviolable, and no inhabitant of the Nation may be deprived of it, except by virtue of a judgment based on law”. The right to property comprises the universality of tangible and intangible assets that form part of a person's patrimony.
22. The Supreme Court of Justice of the Nation of the Argentine Republic (“Supreme Court”) has established that the right to property “protects everything that forms part of the patrimony of the inhabitant of the Nation, be it real or personal rights, tangible or intangible property” (Fallos: 184:137, recital 6). The Supreme Court has also concluded that Articles 14 and 17 of the Argentine Constitution cover “all the appreciable interests that a man may possess outside himself, outside his life and liberty” (Fallos: 344:3476, recital 6; Fallos: 343:1146, recital 8, opinion of Justice Rosatti). Therefore, any right that has a value recognized as such by law, whether it originates in private relations or emanates from administrative acts, is part of the constitutional concept of property.
23. Consequently, all assets, including electronic devices and accounts in messaging applications, and their contents are the exclusive property of their owners. I know of no law that has granted the Defendant the ownership, possession, custody or control of those assets and rights, so that

their seizure would in principle be a direct encroachment on the property of others, with the civil and criminal consequences that could derive from such an act of confiscation.

24. The extensive concept of the right to property is articulated with another fundamental right, the right to privacy, based on the dignity of the human person and also protected in the Argentine Constitution.<sup>8</sup>

25. Indeed, Article 18 of the Argentine Constitution establishes the inviolability of epistolary correspondence and private papers<sup>9</sup>, while Article 19 provides that “[t]he private actions of men that in no way offend public order and morals, nor harm a third party, are reserved to God alone, and are exempt from the authority of the magistrates. No inhabitant of the Nation shall be obliged to do what the law does not command, nor deprived of what the law does not prohibit”.

26. The right to privacy recognized in these norms finds its main safeguard in the right to prevent State interference with that which is personal to each individual, containing his privacy and reflecting his autonomy. State interference in the private sphere of citizens is only justified if it is authorized by law and based on a higher interest that protects the freedom of third parties, the defense of society, good morals or the investigation of a crime (Fallos: 306:1892, recital 8).<sup>10</sup>

---

<sup>8</sup> See also Article 17 of the International Covenant on Civil and Political Rights and Article 11 of the Pact of San José, Costa Rica, both instruments of constitutional hierarchy (Article 75, paragraph 22 of the Argentine Constitution).

<sup>9</sup> Art. 18, Constitution of the Argentine Nation: “(...) The home is inviolable, as well as epistolary correspondence and private papers; and a law shall determine in what cases and with what justification it may be searched and occupied”.

<sup>10</sup> In another ruling (Fallos: 332:1111, recital 24, 2nd par.), the Supreme Court interpreted that the constitutional framework for the protection of privacy also justifies, for example and on an exceptional basis, the use of telephone records for the purposes of a criminal investigation, which must be issued by a competent Argentine judge by means of a well-founded decision.

27. The impact of technology, which generated new means, platforms and communication devices, has also produced the evolution of the concept of privacy and the notions of “private papers” and “epistolar correspondence” of Article 18 of the Constitution, giving a more precise scope to the protection by the State. This is confirmed by the incorporation in the Criminal Code of the Argentine Nation (“Criminal Code”) of specific offenses that punish conduct involving unlawful interference, as will be discussed in subsequent paragraphs.<sup>11</sup>
28. The communications of officials (former and current) contained within their privately-owned devices and non-governmental messaging applications are presumed to be private and subject to the protection of Articles 18 and 19 of the Argentine Constitution.
29. Any action that restricts the right to privacy must be expressly and exhaustively authorized in a law that guarantees due process to the person affected by such limitation.<sup>12</sup> I am not aware of the existence of any law that, outside a criminal proceeding before Argentine courts, authorizes the National State to access or intrude in any way into the private means of communication of its officials. Therefore, the Defendant could not access such communications without directly violating the Argentine Constitution.

---

*See* Art. 236, Code of Criminal Procedure of the Nation: “Under the same conditions, the judge may also order the obtaining of the records of the communications of the accused or of those who communicate with him.

In the cases in which any of the crimes provided for in Articles 142 bis and 170 of the NATIONAL CRIMINAL CODE are being investigated, or which are being processed in connection with them, when there is a duly justified danger in the delay, these powers may be exercised by the judge, such powers may be exercised by the representative of the PUBLIC PROSECUTOR'S OFFICE, by means of a well-founded order, with immediate communication to the Judge, who shall validate it within a non-extendable term of twenty-four hours, under penalty of nullity of the act and consequent ineffectiveness of the evidence introduced from it.”

<sup>11</sup> See GELLI, M. A., *Constitución de la Nación Argentina Comentada y Concordada*, 5th expanded and updated edition, Buenos Aires, La Ley, 2018, , Volume I., pp. 441-442, 480-490.

<sup>12</sup> This interpretation was incorporated in General Comment No. 16 of the United Nations Human Rights Committee, which stated that the obligations imposed by Article 17 of the International Covenant on Civil and Political Rights require States to adopt “legislative and other measures to give effect to the prohibition of such interference and attacks and the protection of this right. It was further stated that the relevant legislation must specify “in detail the precise circumstances in which such interference may be authorized”.

**B. Accessing private devices or private communications without legal authorization is a crime under the Argentine Criminal Code.**

30. Access to private devices (or their contents) without legal authorization would violate the legal order and expose public officials who do so to criminal sanctions. Under the Argentine regulatory system, the actions of public officials must be in accordance with the jurisdiction attributed to them by the legal system. Therefore, public officials may only act when they are expressly or implicitly authorized by law.<sup>13</sup> In other words, the powers of a public official cannot arise from their will: they must be predetermined by a legal rule to which they must necessarily adjust their conduct.<sup>14</sup>

31. Any public official who accesses or takes possession of the personal devices or accounts of the individuals identified by the Plaintiffs would be guilty of the crimes defined in Articles 153<sup>15</sup> and 153 bis<sup>16</sup> of the Criminal Code (Violation of Secrets and Privacy - Second Book, Title V, Chapter II). The criminal conduct included in the criminal type consists of accessing without authorization —or exceeding the authorization one has— to a restricted access computer

---

<sup>13</sup> BARRA, R., Tratado de Derecho Administrativo, Buenos Aires, Editorial Astrea, 2003, Tomo 2, pp.203-206.

<sup>14</sup> CASSAGNE, J. C., Derecho Administrativo, Lima, Editorial Palestra, 2010, Tomo I, pp. 269-270.

<sup>15</sup> Art. 153 of the Criminal Code of the Nation: “Whoever unduly opens or accesses an electronic communication, a letter, a sealed sheet, a telegraphic, telephonic or other type of dispatch that is not addressed to him, or unduly takes possession of an electronic communication, a letter, a sheet, a dispatch or other private paper, even if it is not sealed, or unduly deletes or diverts from its destination a correspondence or an electronic communication that is not addressed to him, shall be punished with imprisonment of fifteen (15) days to six (6) months.

The same penalty shall be incurred by whoever unduly intercepts or captures electronic communications or telecommunications coming from any private or restricted access system.

The penalty shall be imprisonment from one (1) month to one (1) year, if the perpetrator also communicates to another or publishes the content of the letter, writing, dispatch or electronic communication.

If the act is committed by a public official who abuses his functions, he shall also suffer special disqualification for twice the term of the sentence” (emphasis added).

<sup>16</sup> Article 153 bis of the Criminal Code of the Nation: “- Whoever knowingly accesses by any means, without due authorization or exceeding the authorization he has, to a restricted access computer system or data, shall be punished with imprisonment from fifteen (15) days to six (6) months, unless a more severely punishable offense results.

The penalty shall be from one (1) month to one (1) year of imprisonment when the access was to the detriment of a computer system or data of a public state agency or of a provider of public services or financial services.”

system or data. It is important to note that the penalty is aggravated in the case of public officials who commit the unlawful action.

32. The public official who seizes the devices and personal email accounts of the persons identified by the Plaintiffs (current and former public officials) —including collecting their content to deliver them to an external provider or the Defendant's lawyers— without a law or without the order of a competent Argentine judge to do so would incur in the crimes defined in Articles 153 and 153 bis of the Criminal Code. Thus, it would be an encroachment on the rights of property, privacy and intimacy, affecting the “inviolability of private papers” and would result in the direct criminal liability of the public official who unduly interferes and breaches of obligations assumed by the Argentine Republic in international conventions. Even if the Defendant had possession, custody or control of the devices and personal messaging application accounts of the persons identified by the Plaintiffs —which I rule out for the reasons set forth above—, their content would not constitute acts of government as set forth in section II of this report and therefore would not constitute public information covered by the DAIP.

### **III. CONCLUSION**

33. The emails and internal documents are in the nature of conversations, messages or communications that do not manifest acts of government and therefore cannot not be identified as public information. In the event that they were considered to constitute public information, the Defendant would be exempted from the obligation to turn them over if their content is related to any of the matters included in Article 8 of Law 27,275.
34. Pursuant to Articles 17, 18 and 19 of the Argentine Constitution, Defendant does not have and cannot take possession, custody, or control and, therefore, cannot access devices owned by officials (current and former). The Defendant's officials lack the authority to seize personal

messaging devices or applications, and therefore an official who improperly seizes or accesses them would commit the criminal offenses of Articles 153 and 153 bis of the Criminal Code.

35. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: September 18, 2024

---

Miriam Ivanega

**THE FOREGOING IS A TRUE AND ACCURATE TRANSLATION** into English of the attached document in Spanish, which I had before me. Digitally signed in the City of Buenos Aires, Argentina, on September 18, 2024. -----

Juan Manuel Falabella  
Sworn Translator  
English Language  
Registered at the Buenos Aires Sworn Translators' Association  
(Registration No. 7210, Volume XIX, Page 082)



TRIBUNAL DE DISTRITO DE LOS ESTADOS UNIDOS  
DISTRITO DEL SUR DE NUEVA YORK

----- x

PETERSEN ENERGÍA INVERSORA,	:	
S.A.U. Y PETERSEN ENERGÍA,	:	
S.A.U.	:	
	:	
Demandantes,	:	
	:	Caso N° 1:15-cv-02739-LAP
c.	:	
	:	
REPÚBLICA ARGENTINA E YPF	:	
S.A.,	:	
	:	
Demandados.	:	

----- x

ETON PARK CAPITAL	:	
MANAGEMENT, L.P., ETON PARK	:	
MASTER FUND, LTD. Y ETON	:	
PARK FUND, L.P.,	:	
	:	
Demandantes,	:	
	:	Caso N° 1:16-cv-08569-LAP
c.	:	
	:	
REPÚBLICA ARGENTINA E YPF	:	
S.A.,	:	
	:	
Demandados.	:	

----- x

**DECLARACIÓN EXPERTO DE MIRIAM MABEL IVANEGA**

De acuerdo al 28 U.S.C. § 1746 y la Regla 44.1 de las Reglas Federales de los Procedimientos Civiles, yo, Miriam Ivanega, declaro lo siguiente:

1. Los abogados de la República Argentina (la “Demandada”) han solicitado mi opinión sobre ciertas cuestiones de derecho argentino relevantes a una disputa entre la Demandada y los

demandantes Petersen Energía Inversora, S.A.U. y Petersen Energía, S.A.U. (conjuntamente, “Petersen”), y Eton Park Capital Management, L.P., Eton Park Master Fund, Ltd. y Eton Park Fund, L.P. (conjuntamente, “Eton Park” y junto con Petersen, los “Demandantes”) en el proceso de “*discovery*” posterior a la sentencia de primera instancia en los casos arriba mencionados.

2. Soy abogada debidamente licenciada y habilitada en la Argentina. Soy profesora de las materias de Organización Administrativa y Empleo Público y Transparencia, Compliance y Control Público de las Contrataciones Públicas y directora de la Maestría en Derecho Administrativo en la Facultad de Derecho de la Universidad Austral en la Ciudad Autónoma de Buenos Aires, Argentina.
3. Soy Magister en Derecho Administrativo y Doctora en Derecho y Ciencias Sociales, Miembro Fundador del Foro Iberoamericano de Derecho Administrativo y de la Asociación Internacional de Derecho Administrativo y profesora de posgrados en Derecho y conferencista en universidades públicas y privadas de la República Argentina y en otros países de Latinoamérica (Perú, Ecuador, Colombia, Brasil, Uruguay, México, República Dominicana, El Salvador). He publicado once libros vinculados al derecho público, sobre temas de control público, transparencia en las contrataciones públicas, responsabilidad de los funcionarios públicos, organización administrativa y función pública, administración financiera y gestión pública. Entre las funciones ejercidas en el sector público, destaco haber ocupado el cargo de Autoridad de Aplicación de la Ley de Ética Pública en el Consejo de la Magistratura del Poder Judicial de la Ciudad Autónoma de Buenos Aires.

### **RESUMEN EJECUTIVO**

4. Entiendo que los Demandantes han solicitado que la Demandada recopile y entregue ciertos documentos relativos a la relación entre la Demandada e YPF S.A. (“YPF”) o el Banco Central de la República Argentina (“BCRA”), incluyendo comunicaciones de ciertas personas que son o fueron funcionarios del gobierno nacional.
5. En la primera sección de este informe analizo bajo derecho argentino si los correos electrónicos y documentos internos creados o intercambiados entre funcionarios del gobierno argentino involucrando distintos dispositivos bajo la posesión, control o custodia del gobierno nacional constituyen información pública a la que personas ajenas a la administración tengan derecho a acceder. En primer lugar, la Demandada da forma a sus actos cumpliendo con un detallado plexo normativo. Cualquier manifestación o actividad que no se ajuste a dichas normas -incluyendo los correos y documentos internos- constituyen actos deliberativos que no revisten el carácter de actos de gobierno y por ende no constituyen “información pública” según tales conceptos se definen en el derecho argentino. Solo en la medida en que el contenido de esas comunicaciones internas da lugar a actos resolutivos y se vuelcan en gestiones de la administración que constan en el único sistema habilitado a esos efectos, el Sistema de Gestión Documental Electrónica (“GDE”), pasan a ser actos de gobierno que, como regla general, constituyen información pública. En segundo lugar, aun suponiendo que comunicaciones y documentos previos a la generación de un acto de gobierno pudieran considerarse información pública, y el contenido quedase volcado en el GDE, el régimen de derecho de acceso a la información pública previsto en la normativa argentina establece ciertas limitaciones a la obligación de la Demandada de entregar información generada por ella o sus funcionarios.

6. En la segunda sección de este informe analizo bajo derecho argentino si la Demandada podría arrogarse la posesión, control o custodia de dispositivos y cuentas personales de personas que son o fueron funcionarios del gobierno nacional. Conforme el derecho argentino, esos dispositivos y cuentas personales, así como cualquier contenido generado en o por medio de ellos, son propiedad privada de dichos funcionarios y la Demandada no tiene posesión, control o custodia de ellos. Bajo la ley argentina, la Demandada no tiene habilitación legal para recopilar o entregar a terceros los dispositivos y cuentas personales sin la autorización expresa del autor de dichos dispositivos y cuentas. Muy por el contrario, cualquier funcionario de la Demandada que accediera o se apoderare de los dispositivos o cuentas personales de sus funcionarios o su contenido incurriría en los delitos previstos en los artículos 153 y 153bis del Código Penal argentino.

**I. LOS CORREOS ELECTRÓNICOS Y DOCUMENTOS INTERNOS CREADOS O INTERCAMBIADOS ENTRE FUNCIONARIOS DEL GOBIERNO ARGENTINO INVOLUCRANDO DISTINTOS DISPOSITIVOS BAJO LA POSESIÓN, CONTROL O CUSTODIA DEL GOBIERNO NACIONAL NO CONSTITUYEN INFORMACIÓN PÚBLICA A LA QUE PERSONAS AJENAS A LA ADMINISTRACIÓN PUEDAN ACCEDER.**

7. Los correos electrónicos intercambiados entre funcionarios del gobierno argentino involucrando dispositivos bajo la posesión, control o custodia del gobierno nacional, así como los documentos de trabajo internos, no constituyen comunicaciones realizadas mediante el sistema habilitado por el Estado Nacional para la gestión de la actividad administrativa y por ello, no pueden considerarse información a la cual terceros tienen acceso bajo la ley argentina de derecho de acceso a la información pública. Tanto el Estado Nacional como los funcionarios identificados tienen un interés legítimo en preservar la confidencialidad de dicha información, y no podrán ser obligados a divulgarla.

**A. Las comunicaciones y documentos internos de los funcionarios argentinos aun cuando involucren dispositivos bajo la posesión, control o custodia del gobierno nacional, no son “información pública”.**

8. Las funciones del Estado se desarrollan a través de procedimientos y procesos judiciales, legislativos o administrativos que deben ceñirse a las regulaciones respectivas. En el caso del poder ejecutivo, el procedimiento administrativo está compuesto por todos los informes, providencias, dictámenes y documentos oficiales en general que sean producto de la gestión administrativa (Ley N° 19.549 modif. por Ley N° 27.742, Decreto N° 1759/1972 modif. por Decreto N° 695/2024, artículos 7 y 8).
9. Los expedientes administrativos tramitan por medios electrónicos, son resueltos con intervención del órgano al que una ley o un decreto hubieren atribuido competencia y se forman con la agregación ordenada de los documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias que deban integrarlos.
10. La forma que deben adoptar las diferentes instancias que reflejan la voluntad del Estado Nacional de generar un acto de gobierno se encuentra establecida por la vía reglamentaria (Decreto N° 336/2017). En la actualidad, las actuaciones administrativas se canalizan a través del GDE que actúa como plataforma para la implementación de la gestión de los expedientes electrónicos (Decreto N° 695/2024, art. 7.c). El GDE fue implementado en el año 2016 “como sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional”. (Decreto N° 561/2016, arts. 1 y 2).
11. En consecuencia, para que un funcionario de la Demandada manifieste la voluntad del Estado argentino ejerciendo las funciones administrativas, incluyendo dar instrucciones o realizar acuerdos con entidades que tienen personalidad jurídica propia (tengan o no participación

accionaria estatal), debe hacerlo en el marco de un procedimiento administrativo tramitado a través del GDE, que es el único sistema habilitado para ello.

12. Únicamente los informes, dictámenes, providencias, resoluciones u otros actos de la Administración que se plasmen en ese régimen procedimental expresan la voluntad de Estado respecto de un acto de gobierno sujeto al régimen de publicidad.<sup>1</sup> El Decreto N° 333/1985 — luego reemplazado por el Decreto N° 336/2017 en atención a las modificaciones tecnológicas derivadas del uso de GDE— dispuso expresamente que no se daría curso a ningún tipo de documentación que no se ajustare a las normas dispuestas a esos efectos. A los efectos de la administración pública (y la creación de actos de gobierno) todas esas actuaciones no son relevantes. Los correos electrónicos y los documentos creados o compartidos que se intercambien entre funcionarios del gobierno argentino involucrando distintos dispositivos bajo la posesión, control o custodia del gobierno nacional, en la medida que no forman parte de un acto de la administración volcado en GDE, constituyen actos deliberativos y papeles de trabajo —meros intercambios— que no pueden ser identificados como información pública.<sup>2</sup>

13. En la República Argentina, bajo el régimen de acceso a la información pública, las personas únicamente tienen el derecho de solicitar y obtener documentos del gobierno nacional

---

<sup>1</sup> Ver SACRISTÁN, E. B., *Acceso a la información: a propósito de los casos “PAMI” y “Giustiniani”*, JA 2016-I, p. 31. La autora entiende que la normativa de acceso a la información pública se encuentra acotada a los emisores de actos de gobierno. Asimismo, refiere al principio de “publicidad de los actos de gobierno” y su vínculo con el sistema republicano, representativo y federal establecido en el artículo 1 de la Constitución Argentina (cfr. GELLI, M. A., *Constitución de la Nación Argentina Comentada y Concordada*, 5ta edición ampliada y actualizada, Buenos Aires, La Ley, 2018, , T.I., pp. 27-29).

<sup>2</sup> El Decreto N° 780/2024, que modificó el Decreto N° 206/2017 confirma el sentido de que las deliberaciones preparatorias y papeles de trabajo, así como el examen preliminar de un asunto, no son considerados documentos de carácter público.

respecto de actos de gobierno a través de una solicitud de información bajo el procedimiento establecido por la Ley N° 27.275 de Derecho de Acceso a la Información Pública y el Decreto reglamentario N° 206/2017(“DAIP”).<sup>3</sup>

14. El DAIP encuentra sus bases en la concepción que considera al acceso a la información pública respecto de actos de gobierno como derecho fundamental -parte integrante de la libertad de expresión- de todos los ciudadanos que deseen buscar y recibir información y datos en manos del Estado.<sup>4</sup> En consecuencia, la Ley N° 27.275 establece la obligación de la Demandada de entregar documentación respecto de actos de gobierno en respuesta a un pedido efectuado por un ciudadano en ejercicio del DAIP siempre y cuando se refiera a *información pública* (Ley N° 27.275, artículos 2 y 13).
15. Bajo el derecho argentino, a los efectos de la administración pública nacional, *información pública* se predica de todo tipo de dato contenido en documentos de cualquier formato que los funcionarios de dicha administración los sujetos obligados a dar información generen, obtengan, transformen, controlen o custodien en el marco de la actividad estatal. Hasta que no se verifica un acto de gobierno, no hay información pública.
16. Una simple lectura exegética de la Ley N° 19.549 modif. por Ley N° 27.742 y su Decreto Reglamentario (Decreto N° 1759/1972, modif. por Decreto N° 695/2024), el Decreto N° 336/2017 y el Decreto N° 561/2016, muestra que los correos electrónicos internos intercambiados entre funcionarios del gobierno argentino involucrando dispositivos bajo la

---

<sup>3</sup> Esto es sin perjuicio de las facultades jurisdiccionales en el marco de los procesos penales.

<sup>4</sup> Ver Artículos 1, 14, 16, 31, 32 y 33 de la Constitución Argentina; Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos y de la Declaración Universal de Derechos Humanos, Artículo 13 de la Convención Americana sobre Derechos Humanos y Artículo 4 de la Declaración Americana de los Derechos y Deberes del Hombre.

posesión, control o custodia del gobierno nacional, así como los documentos de trabajo internos que no estén volcados al sistema GDE y no constituyen actos de gobierno no tienen carácter de información pública. En consecuencia, la Demandada no se encuentra obligada a entregar esos documentos. Dicha obligación solo existirá en la medida que el contenido de esas comunicaciones o documentos internos se vuelque en un informe, dictamen, providencia, resolución u otros actos de gobierno a través del sistema GDE.

**B. Incluso si las comunicaciones y documentos internos del gobierno que involucrasen dispositivos bajo la posesión, control o custodia del gobierno nacional pudieran considerarse información pública, la Demandada se encuentra exceptuada de su obligación de entrega de cualquier información alcanzada por las excepciones previstas en la Ley de Derecho de Acceso a la Información Pública.**

17. Aun suponiendo que comunicaciones intercambiadas o documentos elaborados involucrando dispositivos bajo la posesión, control o custodia del gobierno nacional y otros documentos internos pueden ser considerados actos de gobierno, el mismo régimen de DAIP establece que cierta información no está sujeta a la divulgación pública.

18. La Demandada no está obligada a divulgar bajo el DAIP información privilegiada (excluida del régimen) por vincularse con las materias excluidas del acceso al público establecidas en el artículo 8 de la Ley N° 27.275. Esas restricciones legítimas son:

- a. Información expresamente clasificada como reservada o confidencial o secreta por razones de defensa o política exterior<sup>5</sup>;
- b. Información que pudiera poner en peligro el correcto funcionamiento del sistema financiero o bancario;
- c. Los secretos industriales, comerciales, financieros, científicos, técnicos o tecnológicos cuya revelación pudiera perjudicar el nivel de competitividad o lesionar sus intereses;

---

<sup>5</sup> La defensa o la política exterior se vinculan con la seguridad nacional, en sentido amplio, razón que en un Estado ha de constituir una legítima restricción al derecho de acceso a la información pública, siempre que se establezca por ley.



- d. Información que comprometa los derechos o intereses legítimos de un tercero obtenida en carácter confidencial;
- e. Información en poder de la Unidad de Información Financiera tendiente a la prevención e investigación de activos provenientes de ilícitos;
- f. Información elaborada por quienes se encuentran dedicados a regular o supervisar instituciones financieras cuando se refieran a exámenes de situación, evaluación de su sistema de operación o condición de su funcionamiento;
- g. Información elaborada por asesores jurídicos o abogados de la administración pública nacional cuya publicidad pudiera revelar la estrategia a adaptarse en la defensa o tramitación de una causa judicial o divulgare las técnicas o procedimientos de investigación de algún delito u otra irregularidad o cuando la información privare a una persona del pleno ejercicio de la garantía del debido proceso;
- h. Información protegida por el secreto profesional;
- i. Información que contenga datos personales (cfr. Ley N° 25.326 de Protección de Datos Personales);<sup>6</sup>
- j. Información que pueda ocasionar un peligro a la vida o seguridad de una persona;
- k. Información de carácter judicial cuya divulgación estuviera vedada por otras leyes o por compromisos contraídos por la Demandada en tratados internacionales;
- l. Información obtenida en investigaciones que tuviera el carácter de reservada y cuya divulgación pudiera frustrar el éxito de una investigación; e
- m. Información correspondiente a una sociedad anónima sujeta al régimen de oferta pública.

19. Frente a un pedido efectuado por una persona en ejercicio del DAIP que caiga bajo alguna de las excepciones establecidas en el artículo 8 de la Ley N° 27.275, el Estado se encuentra exceptuado de la obligación de proveer información.<sup>7</sup>

---

<sup>6</sup> El artículo 5 de la Ley N° 25.326 precisa como principio que el tratamiento de datos personales es ilícito cuando no hubiera consentimiento del titular. En forma consecuente, el artículo 7 establece que nadie puede ser obligado a proporcionar datos sensibles, estableciéndose únicamente dos excepciones a este principio: cuando medien razones de interés general autorizadas por ley o cuando su uso está vinculado con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

<sup>7</sup> El único supuesto en el que estas excepciones no son aplicables, es el previsto, expresamente, en el artículo 8 último párrafo y refiere a “casos de graves violaciones de derechos humanos, genocidio, crímenes de guerra o delitos de lesa humanidad”

**II. LA DEMANDADA NO TIENE NI PUEDE ARROGARSE POSESION, CONTROL O CUSTODIA DE LOS DISPOSITIVOS Y CUENTAS PERSONALES DE FUNCIONARIOS (ACTUALES Y ANTERIORES) DEL GOBIERNO ARGENTINO.**

**A. En ausencia de una ley del Congreso o una orden judicial de un tribunal argentino que lo autorice, la República Argentina no puede acceder a los dispositivos privados ni a las comunicaciones privadas de sus ciudadanos sin violar directamente la Constitución Nacional.**

20. Los dispositivos (con su contenido) y las cuentas de correo electrónicos personales a las que buscan acceso las Demandantes no están en posesión de, ni están bajo el control o custodia de la Demandada. Por el contrario, son de exclusiva propiedad de sus titulares. Tanto esos dispositivos como su contenido —en tanto no haya sido hecho público por sus legítimos propietarios— constituyen para la Demandada propiedad ajena.
21. El artículo 17 de la Constitución Nacional (“Constitución Argentina”) prevé que “[l]a propiedad es inviolable, y ningún habitante de la Nación puede ser privado de ella, sino en virtud de sentencia fundada en ley”. El derecho de propiedad comprende la universalidad de bienes materiales e inmateriales que forman parte del patrimonio de una persona.
22. La Corte Suprema de Justicia de la Nación de la República Argentina (“Corte Suprema”) ha establecido que el derecho de propiedad “ampara todo aquello que forma el patrimonio del habitante de la Nación, trátase de derechos reales o personales, de bienes materiales o inmateriales” (Fallos: 184:137, considerando 6). La Corte Suprema también ha concluido que los artículos 14 y 17 de la Constitución Argentina abarcan “todos los intereses apreciables que un hombre puede poseer fuera de sí mismo, fuera de su vida y de su libertad” (Fallos: 344:3476, considerando 6; Fallos: 343:1146, considerando 8, voto del Juez Rosatti). Por lo tanto, todo derecho que tenga un valor reconocido como tal por la ley, sea que se origine en

las relaciones privadas o que emane de actos administrativos, forma parte del concepto constitucional de propiedad.

23. En consecuencia, todos los bienes, entre ellos los dispositivos electrónicos y las cuentas en aplicaciones de mensajería, y su contenido son de exclusiva propiedad de sus titulares. No conozco ley que haya otorgado a la Demandada la titularidad, posesión, custodia o control de aquellos bienes y derechos, por lo que su apoderamiento implicaría en principio un avasallamiento directo a la propiedad ajena, con las consecuencias civiles y penales que podrían derivarse de tal acto de confiscación.

24. El concepto extensivo del derecho de propiedad se articula con otro derecho fundamental, el derecho a la privacidad, sustentado en la dignidad de la persona humana y protegido también en la Constitución Argentina.<sup>8</sup>

25. En efecto, el artículo 18 de la Constitución Argentina establece la inviolabilidad de la correspondencia epistolar y los papeles privados<sup>9</sup> mientras que el artículo 19 dispone que “[l]as acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe”.

---

<sup>8</sup> Ver también el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y el artículo 11 del Pacto de San José de Costa Rica, ambos instrumentos de jerarquía constitucional (art. 75, inc. 22 de la Constitución Argentina).

<sup>9</sup> Art. 18, Constitución de la Nación Argentina: “(...) El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación”.

26. El derecho a la privacidad reconocido en estos preceptos encuentra su principal resguardo en el derecho a impedir la interferencia del Estado con aquello que es personal de cada individuo, conteniendo a su intimidad y reflejo de su autonomía. La intromisión estatal en la esfera privada de los ciudadanos sólo se justifica si está avalada por una ley y en función de un interés superior que resguarda la libertad de los terceros, la defensa de la sociedad, las buenas costumbres o la investigación de un delito (Fallos: 306:1892, considerando 8).<sup>10</sup>
27. El impacto de la tecnología, que generó nuevos medios, plataformas y dispositivos de comunicación ha producido también la evolución del concepto de privacidad y de las nociones de “papeles privados” y “correspondencia epistolar” del artículo 18 de la Constitución, otorgando un alcance más preciso a la protección por parte del Estado. Esto se confirma con la incorporación en el Código Penal de la Nación Argentina (“Código Penal”) de delitos específicos que castigan conductas que implican una intromisión ilegítima, tal como se analizará en párrafos posteriores.<sup>11</sup>

---

<sup>10</sup> En otra sentencia (Fallos: 332:1111, considerando 24, 2do par.), la Corte Suprema interpretó que el marco constitucional protectorio de la privacidad también justifica, por ejemplo y con carácter excepcional, la utilización del registro de comunicaciones telefónicas a los fines de una investigación penal, la cual requiere ser emitida por un juez argentino competente mediante una decisión fundada.

Ver Art. 236, Código Procesal Penal de la Nación: “Bajo las mismas condiciones, el Juez podrá ordenar también la obtención de los registros que hubiere de las comunicaciones del imputado o de quienes se comunicaran con él. En las causas en que se investigue alguno de los delitos previstos en los artículos 142 bis y 170 del CODIGO PENAL DE LA NACION, o que tramiten en forma conexa con aquéllas, cuando existiese peligro en la demora, debidamente justificado, dichas facultades podrán ser ejercidas por el representante del MINISTERIO PUBLICO FISCAL, mediante auto fundado, con inmediata comunicación al Juez, quien deberá convalidarla en el término improrrogable de veinticuatro horas, bajo pena de nulidad del acto y consecuente ineficacia de la prueba introducida a partir de él.”

<sup>11</sup> Ver GELLI, M. A., Constitución de la Nación Argentina Comentada y Concordada, 5ta edición ampliada y actualizada, Buenos Aires, La Ley, 2018, , T.I., pp. 441-442, 480-490.

28. Las comunicaciones de los funcionarios (anteriores y actuales) contenidas dentro de los dispositivos de su propiedad y aplicaciones de mensajería no gubernamentales se presumen privadas y sujetas a la protección de los artículos 18 y 19 de la Constitución Argentina.
29. Toda acción que restrinja el derecho a la privacidad debe estar prevista de forma expresa y taxativa en una ley que garantice el debido proceso de la persona afectada por esa limitación.<sup>12</sup> No conozco la existencia de ley que, por fuera de un proceso penal ante tribunales argentinos, autorice al Estado Nacional a acceder o inmiscuirse de cualquier manera en los medios de comunicación privados de sus funcionarios. Por lo tanto, la Demandada no podría acceder a tales comunicaciones sin violar directamente la Constitución Argentina.

**B. El acceso a los dispositivos privados o a las comunicaciones privadas sin autorización legal es delito bajo el Código Penal argentino.**

30. El acceso a los dispositivos privados (o su contenido) sin autorización legal vulneraría el orden legal y exponería a los funcionarios públicos que lo hicieran a sanciones penales. Bajo el sistema normativo argentino, la actuación de los funcionarios públicos debe ajustarse a la competencia atribuida por el ordenamiento jurídico. Por eso los funcionarios públicos únicamente pueden actuar cuando están expresa o implícitamente autorizados por la normativa.<sup>13</sup> En otras palabras, las atribuciones de un funcionario no pueden surgir de su

---

<sup>12</sup> Esa interpretación se incorporó en la Observación General N° 16 del Comité de Derechos Humanos de la Organización de las Naciones Unidas, donde se señaló que las obligaciones impuestas por el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos exigen que los Estados adopten “medidas legislativas y de otra índole para hacer efectivas la prohibición de esas injerencias y ataques y la protección de este derecho”. Incluso, se expresó que la legislación pertinente debe especificar “con detalle las circunstancias precisas en que podrán autorizarse esas injerencias”.

<sup>13</sup> BARRA, R., Tratado de Derecho Administrativo, Buenos Aires, Editorial Astrea, 2003, Tomo 2, pp.203-206.

voluntad: han de estar predeterminadas por una norma jurídica a la cual debe ajustarse, obligatoriamente, su conducta.<sup>14</sup>

31. Aquel funcionario público que accediera o se apoderare de los dispositivos o cuentas personales de los individuos identificados por las Demandantes incurriría en los delitos definidos en los artículos 153<sup>15</sup> y 153 bis<sup>16</sup> del Código Penal (Violación de Secretos y de la Privacidad-Libro Segundo, Título V, Capítulo II). La conducta típica incluida en el tipo penal consiste en acceder sin autorización —o excediendo la que se tiene— a un sistema o dato informático de acceso restringido. Es importante notar que la pena se agrava en caso de ser funcionarios públicos quienes cometen la acción ilícita.

32. El funcionario público que se apoderare de los dispositivos y cuentas de correos electrónicos personales de las personas identificadas por las Demandantes (funcionarios públicos actuales y anteriores) —incluyendo recopilar su contenido para entregarlos a un proveedor externo o los abogados de la Demandada— sin una ley o sin la orden de juez argentino competente que lo habilite incurriría en los delitos definidos en los artículos 153 y 153 bis del Código Penal.

---

<sup>14</sup> CASSAGNE, J. C., Derecho Administrativo, Lima, Editorial Palestra, 2010, Tomo I, pp. 269-270.

<sup>15</sup> Art. 153 del Código Penal de la Nación: “Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o capture comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá, además, inhabilitación especial por el doble del tiempo de la condena” (el remarcado me pertenece).

<sup>16</sup> Art. 153 bis del Código Penal de la Nación: “Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.”

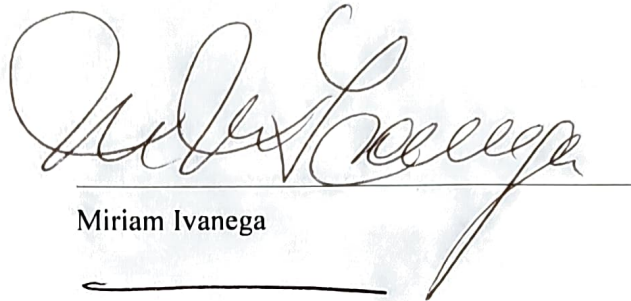
Así, se trataría del avasallamiento de los derechos de propiedad, privacidad e intimidad, afectando la “inviolabilidad de los papeles privados” y derivaría en la responsabilidad penal directa del funcionario público que se inmiscuya indebidamente e incumplimientos de obligaciones asumidas por la República Argentina en convenciones internacionales. Incluso si la Demandada tuviera la posesión, custodia o control de los dispositivos y cuentas de aplicaciones de mensajería personales de las personas identificadas por las Demandantes — lo que descarto por las razones expuestas *supra*—, su contenido no constituiría actos de gobierno conforme lo dispuesto en la sección II de este informe y por ende no constituiría información pública alcanzada por el DAIP.

### III. CONCLUSIÓN

33. Los correos electrónicos y los documentos internos revisten carácter de conversaciones, mensajes o comunicaciones que no manifiestan actos de gobierno por lo que no podrían identificarse como información pública. En el supuesto que se considerase que constituyen información pública, la Demandada se encontraría exenta de la obligación de entregarlos si su contenido se relaciona con algunas de las materias incluidas en el artículo 8 de la Ley 27.275.
34. En virtud de los artículos 17, 18 y 19 de la Constitución Argentina, la Demandada no tiene ni puede arrogarse la posesión, custodia, ni el control y, por lo tanto, no puede acceder a los dispositivos que son propiedad de funcionarios (actuales y anteriores). Los funcionarios de la Demandada carecen de competencia para apoderarse de los dispositivos o aplicaciones de mensajería personal, por lo que un funcionario que indebidamente se apodere o acceda a ellos incurriría en las figuras delictivas de los artículos 153 y 153 bis del Código Penal.

35. Declaro bajo pena de perjurio de conformidad con las leyes de los Estados Unidos de América que lo anterior es verdadero y correcto.

Fecha: 18 de septiembre de 2024



Miriam Ivanega